

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

CHRISTINA MOYER,)	
)	
Plaintiff,)	Case No. 14-cv-561
)	
v.)	Hon. Elaine Bucklo
)	
MICHAELS STORES, INC.,)	
)	
Defendant.)	

MICHAEL C. GOUWENS and JESSICA E. GOUWENS, individually and on behalf of a class,)	
)	
Plaintiffs,)	Case No. 14-cv-648
)	
v.)	Hon. Edmond E. Chang
)	
MICHAELS STORES, INC., a Delaware corporation,)	
)	
Defendant.)	

NANCY MAIZE and JESSICA GORDON, individually and on behalf of all others similarly situated,)	
)	
Plaintiffs,)	Case No. 14-cv-1229
)	
v.)	Hon. John J. Tharp
)	
MICHAELS STORES, INC., a Delaware corporation,)	
)	
Defendant.)	

DANIEL RIPES, individually and on behalf)	
of all others similarly situated,)	
)	Case No. 14-cv-1827
Plaintiff,)	
)	Hon. Ruben J. Castillo
v.)	
)	
MICHAELS STORES, INC., a Delaware)	
corporation,)	
)	
Defendant.)	

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Christina Moyer, Michael C. Gouwens, Jessica E. Gouwens, Nancy Maize, Daniel Ripes, and Mary Jane Whalen (“Plaintiffs”), bring this Consolidated Class Action Complaint against Defendant Michaels Stores Inc. (“Defendant” or “Michaels”), individually and on behalf of all others similarly situated, and complain and allege upon personal knowledge as to themselves and their own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Michaels for its failure to secure and safeguard its customers’ personal financial data, including credit and debit card information.

2. On January 25, 2014, Michaels initially disclosed a possible data breach involving the theft of customers’ credit-card and debit-card data (the “Security Breach”). While the existence of the breach was allegedly uncertain to Defendant, Michaels had previously been alerted to “possible fraudulent activity on some U.S. payment cards that had been used at Michaels.”¹

¹ Chuck Rubin, *A Letter From Our CEO*, Michaels (Jan. 25, 2014), <http://www.michaels.com/corporate/payment-card-notice,default,pg.html>.

3. On April 17, 2014, Michaels CEO Chuck Rubin confirmed the Security Breach and divulged more details regarding its breadth and scope.² Reportedly, approximately 3 million customers had their personal information compromised by the breach when making purchases at both Michaels stores and Aaron Brothers stores, a subsidiary of Michaels.

4. Michaels' security failures enabled the hackers to steal financial data from within Michaels' stores and subsequently make unauthorized purchases on customers' credit cards and otherwise put Class members' financial information at serious and ongoing risk. The hackers continue to use the information they obtained as a result of Michaels' inadequate security to exploit and injure Class members across the United States.

5. The Security Breach was caused and enabled by Michaels' knowing violation of its obligations to abide by best practices and industry standards in protecting customers' personal information. Michaels grossly failed to comply with security standards and allowed their customers' financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

6. Michaels failed to disclose the extent of the Security Breach and notify its affected customers of the Breach in a timely manner. Michaels failed to take other reasonable steps to clearly and conspicuously inform its customers of the nature and extent of the Security Breach. Furthermore, by failing to provide adequate notice, Michaels prevented Class members from protecting themselves from the Security Breach.

7. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class, assert claims for breach of implied contract, violation of the Illinois Consumer Fraud and

² Chuck Rubin, *A Letter From Our CEO*, Michaels (Apr. 17, 2014), <http://www.michaels.com/corporate/payment-card-notice-CEO,default.pg.html>.

Deceptive Business Practices Act, 815 ILCS 505/1, *et seq.*, and violation of the New York General Business Law § 349, and seek injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

8. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). In the aggregate, Plaintiffs' claims and the claims of the other members of the Class exceed \$5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of States other than Michaels' state of citizenship.

9. This Court has personal jurisdiction over Michaels because Michaels is registered with the Illinois Secretary of State to conduct business in the State of Illinois, and does conduct substantial business in the State of Illinois, such that Michaels has significant continuous and pervasive contacts with the State of Illinois. Michaels also maintains numerous stores and employees in the State of Illinois, including multiple stores compromised in the Security Breach.

10. Venue is proper in this District pursuant to 28 U.S.C. §§ 1301(a)(2), 1391(b)(2), and 1391(c)(2) as: a substantial part of the events and/or omissions giving rise to the claims emanated from activities within this District, and Michaels conducts substantial business in this District.

III. PARTIES

Plaintiff Moyer

11. Christina Moyer is citizen of the State of Illinois and is domiciled in Cook County, Illinois. Moyer made purchases with her debit card at a Michaels retail location in Cook County, Illinois on December 9, 2013. As a result, Moyer entered into an implied contract with Michaels for the adequate protection of her debit card information, and had her sensitive

financial information exposed as a result of Michaels' inadequate security. Following the Data Breach, Moyer purchased credit monitoring protection to mitigate her harm.

Plaintiffs Gouwens

12. Plaintiffs Michael C. Gouwens and Jessica E. Gouwens are citizens of the State of Illinois and are domiciled in Lake County, Illinois. The Gouwens made purchases with a credit card at a Michaels retail location in Kildeer, Illinois, on December 5 and 11, 2013, as well as January 16, 2014. As a result, the Gouwens entered into an implied contract with Michaels for the adequate protection of their credit card information and had their sensitive financial information exposed as a result of Michaels' inadequate security.

Plaintiff Maize

13. Nancy Maize is a citizen of Illinois and is domiciled in Cook County, Illinois. Maize made purchases with her debit card at a Michaels retail location in Skokie, Illinois on December 13, 2013. As a result, Maize entered into an implied contract with Michaels for the adequate protection of her debit card information and had her sensitive financial information exposed as a result of Michaels' inadequate security.

Plaintiff Ripes

14. Daniel Ripes is a citizen of the State of Illinois and is domiciled in Lake County, Illinois. Ripes made purchases with his credit card at a Michaels retail location in Glenview, Illinois, on November 3, 2013, as well as at a Michaels retail location in Vernon Hills, Illinois, on December 28, 2013. As a result, Ripes entered into an implied contract with Michaels for the adequate protection of his credit card information and had his sensitive financial information exposed as a result of Michaels' inadequate security.

Plaintiff Whalen

15. Mary Jane Whalen is a citizen of the State of New York and is domiciled in Nassau County, New York. Whalen made purchases with her credit card at a Michaels retail location in Manhasset, NY, on December 31, 2013. As a result, Whalen entered into an implied contract with Michaels for the adequate protection of her credit card information and had her sensitive financial information exposed as a result of Michaels' inadequate security. Thereafter, on January 14, 2014, Whalen's credit card was physically presented for payment to a gym in Ecuador for a charge of \$398.16. On January 15, 2014, Whalen's credit card was also physically presented for payment to a concert ticket company in Ecuador for a charge of \$1,320.00. Whalen has never been to Ecuador, did not give her card to someone who travelled to Ecuador, and did not authorize for payments to be made in Ecuador. Whalen canceled her card on January 15, 2014. On information and belief, physical presentment of a card is only possible by recreating a credit card with stolen PII, and, therefore, Whalen's card was fraudulently recreated and used in Ecuador.

Defendant Michaels

16. Michaels Stores, Inc. is a Delaware corporation with its principal place of business in Irving, Texas. Michaels is the largest arts and crafts specialty retailer in North America providing materials, project ideas, and education for creative activities.

IV. FACTUAL BACKGROUND

The Data Breach

17. Michaels operates approximately 1,106 retail locations in 49 states and Canada, and Michaels also operates 123 Aaron Brothers stores in nine states. Like many other retailers, Michaels processes in-store debit and credit card payments.

18. At this point, Michaels has confirmed that approximately 3 million consumers became the victims of a data breach when their personal information was taken from Michaels' payment card information systems as a result of malicious software. Approximately 2.6 million cards were compromised at Michaels stores during a breach which lasted almost 9 months from May 8, 2013 to January 27, 2014.

19. Furthermore, approximately 400,000 cards were compromised at various Aaron Brothers stores during a breach lasting around 8 months, from June 26, 2013 to February 27, 2014.

20. Michaels has received reports of fraud from payment card brands and banks relating to the fraudulent use of cards connected to Michaels and Aaron Brothers.³

21. Furthermore, almost *one year* has passed from the beginning of the data breach to Michaels' confirmation of the breach. In addition, nearly three months passed between when Defendant originally notified the public of a possible breach and when Defendant affirmatively confirmed that the Breach occurred.

22. Michaels' failure to comply with reasonable security standards provided Michaels with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the expense and to the severe detriment of Michaels' own customers – including Class members here – who have been subject to the Security Breach or otherwise have had their financial information placed at serious and ongoing risk.

23. Moreover, this breach is the second time in the past three years that Michaels has been the subject of a security breach. The prior incident occurred in May 2011 and should have alerted Michaels of the need for additional security measures.

³ See *supra*, note 2.

24. Michaels allowed widespread and systematic theft of its customers' financial information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' financial information.

Security Breaches Lead to Identity Theft

25. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits, and incur charges and credit in a person's name.⁴ As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

26. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumer's finances, credit history, and reputation and can take time, money, and patience to resolve.⁵ Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.⁶

27. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit

⁴ See <http://www.gao.gov/new.items/d07737.pdf>.

⁵ See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), <http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf> (last visited Dec. 19, 2013).

⁶ The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

28. Personal identifying information (“PII”) – such as Michaels’ customer names combined with their credit or debit card information that were stolen in the Security Breach at issue in this action– is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for a number of years.⁷ As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, and other PII directly on various Internet websites making the information publicly available.

The Monetary Value of Privacy Protections

29. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer’s personal information as follows:

The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it’s something on the order of the life blood, the free flow of information.⁸

⁷ Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation’s Norton brand has created a software application that values a person’s identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. See also T. Soma, ET AL, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009).

⁸ *The Information Marketplace: Merging and Exchanging Consumer Data*, <http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm> (last visited Dec. 20, 2013).

30. Though Commissioner's Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a \$26 billion per year online advertising industry in the United States.⁹

31. The FTC has also recognized that consumer data is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.¹⁰

32. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent, consumers will make a profit from the surrender of their PII.¹¹ This business has created a new market for the sale and purchase of this valuable data.¹²

33. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy

⁹ See *Web's Hot New Commodity: Privacy*, <http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html> (last visited Dec. 20, 2013) ("Web's Hot New Commodity: Privacy").

¹⁰ *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited Dec. 20, 2013).

¹¹ *You Want My Personal Data? Reward Me for It*, <http://www.nytimes.com/2010/07/18/business/18unboxed.html> (last visited Dec. 20, 2013).

¹² See *Web's Hot New Commodity: Privacy*.

information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”¹³

34. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between \$11.33 and \$16.58 per website.¹⁴

35. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ PII has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

36. In addition, members of the payment card industry (“PCI”) established a Security Standards Counsel (“PCI SSC”) in 2006 to develop PCI Data Security Standards (“PCI DSS”) for increased security of payment processing systems.

37. The PCI DSS provides, “PCI DSS applies to all entities involved in payment card processing—including merchants.”¹⁵ Michaels is a merchant that accepts payment cards.

38. The PCI DSS requires a merchant to, among other things, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, and regularly monitor and test networks.

39. On information and belief, Michaels failed to comply with the PCI DSS, resulting in the security breach.

¹³ Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at 2, available at <http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (emphasis added) (last visited Dec. 20, 2013); Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) *Information Systems Research* 254, 254 (June 2011).

¹⁴ *Id.*

¹⁵ *Requirements an Security Assessment Procedures, Version 3.0*, Payment Card Industry Data Security Standard, at 5 (Nov. 2013), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

Damages Sustained By Plaintiffs and the Class

40. A portion of the services purchased from Michaels by Plaintiffs and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiffs and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the Class incurred actual monetary damages in that they overpaid for the products purchased from Michaels.

41. Plaintiffs and the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments, and/or related bank fees charged to their accounts.

42. After the breach, Michaels encouraged consumers to check their credit reports, place holds on their credit reports, file police reports, and close any affected accounts.¹⁶ However, as explained above, fraudulent use of cards might not be apparent for years. Therefore, consumers must expend considerable time taking these precautions for years to come.

43. Despite this protracted period of potential fraud, Michaels offers affected consumers only one year of credit monitoring.¹⁷ As security blogger Brian Krebs notes, “credit monitoring services will do nothing to protect consumers from fraud on existing financial accounts – such as credit and debit cards – and they’re not great at stopping new account fraud committed in your name.”¹⁸ Michaels’ proposed solutions to the potential fraud are, therefore, woefully deficient.

¹⁶ *Additional Information*, Michaels, <http://www.michaels.com/corporate/payment-card-notice-info,default,pg.html> (last visited Mar. 31, 2014).

¹⁷ *See supra*, note 2.

¹⁸ Brian Krebs, *3 Million Customer Credit, Debit Cards Stolen in Michaels, Aaron Brothers Breaches*, Krebs on Security (Apr. 14, 2014), <http://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/#more-25704>.

44. As a result of these activities, Plaintiffs and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Michaels' wrongful conduct, particularly given the incidents of actual misappropriation from Class members' financial accounts, as detailed above.

45. Plaintiffs and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Security Breach. Such damages also include the cost of obtaining replacement credit and debit cards.

V. CLASS ACTION ALLEGATIONS

46. Plaintiffs bring Count I, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rule of Civil Procedure on behalf of a class defined as:

All persons residing in the United States who made an in-store purchase at a Michaels store using a debit or credit card at any time from May 8, 2013 through January 27, 2014, or who made an in-store purchase at a Aaron Brothers store between June 26, 2013 and February 27, 2014 (the "National Class").

Excluded from the National Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

47. Plaintiffs bring Count II, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

All persons residing in one of the Consumer Fraud States¹⁹ who made an in-store purchase at a Michaels store using a debit or

¹⁹ The States that have similar consumer fraud laws based on the facts of this case are: Arkansas (Ark. Code § 4-88-101, *et seq.*); California (Cal. Bus. & Prof. Code §17200, *et seq.* and Cal. Civil Code

credit card at any time from May 8, 2013 through January 27, 2014, or who made an in-store purchase at a Aaron Brothers store between June 26, 2013 and February 27, 2014 (the “Consumer Fraud Multistate Class”).

Excluded from the Consumer Fraud Multistate Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

48. In the alternative to Count II, Plaintiffs bring Count III and IV, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of the following two state sub-classes, defined as:

Count III

All persons residing in the State of Illinois who made an in-store purchase at a Michaels store using a debit or credit card at any time from May 8, 2013 through January 27, 2014, or who made an in-store purchase at a Aaron Brothers store between June 26, 2013 and February 27, 2014 (the “Illinois State Class”).

—and—

Count IV

All persons residing in the State of New York who made an in-store purchase at a Michaels store using a debit or credit card at any time from May 8, 2013 through January 27, 2014, or who made an in-store purchase at a Aaron Brothers store between June 26, 2013 and February 27, 2014 (the “New York State Class”).

§ 1750, *et seq.*); Colorado (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut (Conn. Gen. Stat. § 42-110, *et seq.*); Delaware (Del. Code tit. 6, § 2511, *et seq.*); District of Columbia (D.C. Code § 28-3901, *et seq.*); Florida (Fla. Stat. § 501.201, *et seq.*); Hawaii (Haw. Rev. Stat. § 480-1, *et seq.*); Idaho (Idaho Code § 48-601, *et seq.*); Illinois (815 ICLS § 505/1, *et seq.*); Maine (Me. Rev. Stat. tit. 5 § 205-A, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws § 445.901, *et seq.*); Minnesota (Minn. Stat. § 325F.67, *et seq.*); Missouri (Mo. Rev. Stat. § 407.010, *et seq.*); Montana (Mo. Code. § 30-14-101, *et seq.*); Nebraska (Neb. Rev. Stat. § 59-1601, *et seq.*); Nevada (Nev. Rev. Stat. § 598.0915, *et seq.*); New Hampshire (N.H. Rev. Stat. § 358-A:1, *et seq.*); New Jersey (N.J. Stat. § 56:8-1, *et seq.*); New Mexico (N.M. Stat. § 57-12-1, *et seq.*); New York (N.Y. Gen. Bus. Law § 349, *et seq.*); North Dakota (N.D. Cent. Code § 51-15-01, *et seq.*); Oklahoma (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon (Or. Rev. Stat. § 646.605, *et seq.*); Rhode Island (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Dakota (S.D. Code Laws § 37-24-1, *et seq.*); Virginia (VA Code § 59.1-196, *et seq.*); Vermont (Vt. Stat. tit. 9, § 2451, *et seq.*); Washington (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia (W. Va. Code § 46A-6-101, *et seq.*); and Wisconsin (Wis. Stat. § 100.18, *et seq.*).

Excluded from the Illinois State Class and New York State Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

49. The National Class, Consumer Fraud Multistate Class, Illinois State Class, and New York State Class are collectively referred to as the “Class,” unless specifically indicated otherwise.

50. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

51. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, Class members number in the thousands. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from Michaels’ books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

52. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

- a. Whether Michaels failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers’ sensitive financial information;

- b. Whether Michaels properly implemented its purported security measures to protect customer financial information from unauthorized capture, dissemination, and misuse;
- c. Whether Michaels' conduct violates the Illinois and other asserted Consumer Fraud Acts;
- d. Whether Michaels' conduct constitutes breach of an implied contract;
- e. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

53. Michaels engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

54. **Typicality – Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Michaels' uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Michaels that are unique to Plaintiffs.

55. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent; they have retained counsel competent and experienced in complex class action litigation; and Plaintiffs will prosecute this

action vigorously. The Class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

56. Insufficiency of Separate Actions – Federal Rule of Civil Procedure 23(b)(1).

Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Michaels. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

57. Declaratory and Injunctive Relief – Federal Rule of Civil Procedure 23(b)(2).

Michaels has acted or refused to act on grounds generally applicable to Plaintiffs and the other Class members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

58. Superiority – Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Michaels, so it would be impracticable for Class members to individually seek redress for Michaels' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for

inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED

COUNT I

Breach of Implied Contract (On Behalf of the National Class)

59. Plaintiffs incorporate paragraphs 1-58 as if fully set forth herein.

60. Michaels' customers who intended to make in-store purchases with debit or credit cards were required to provide their card's magnetic strip data for payment verification.

61. In providing such financial data, Plaintiffs and the other members of the Class entered into an implied contract with Michaels whereby Michaels became obligated to reasonably safeguard Plaintiffs' and the other Class members' sensitive, non-public information.

62. Plaintiffs and the Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract.

63. Michaels breached the implied contract with Plaintiffs and the other members of the Class by failing to take reasonable measures to safeguard their financial data.

64. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to loss of their financial information, loss of money, and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II

**Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
(and Substantially Similar Laws of the Consumer Fraud States²⁰)
(on Behalf of the Consumer Fraud Multistate Class)**

65. Plaintiffs incorporate paragraphs 1-58 as if fully set forth herein.

66. Plaintiffs and the other members of the Class were deceived by Michaels' failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while shopping at Michaels.

67. Michaels intended for Plaintiffs and the other members of the Class to rely on Michaels to protect the information furnished to it in connection with their debit and credit card transactions, in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

68. Michaels instead handled Plaintiffs and the other Class members' personal information in such manner that it was compromised.

69. Michaels failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

70. It was foreseeable that Michaels' willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

71. Michaels benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Michaels saved on the cost of those security measures.

²⁰ The Consumer Fraud States were defined at *supra* note 19.

72. Michaels' fraudulent and deceptive acts and omissions were intended to induce Plaintiffs' and the other Class members' reliance on Michaels' deception that their financial information was secure and protected when using debit and credit cards to shop at Michaels.²¹

73. Michaels violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs' and the other members' private financial information, by failing to warn shoppers that their information was at risk, and by failing to immediately notify affected customers of the nature and extent of the security breach.

74. Michaels' acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

75. Michaels' conduct constitutes unfair acts or practices as defined in that statute because Michaels caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

76. In addition, Michaels also engaged in an unlawful practice by failing to comply with 815 ILCS 530/10(a), which provides:

Sec. 10. Notice of Breach. (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system

77. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

²¹ The consumer protection statutes or interpretive law of the Consumer Fraud States have also either: (a) expressly prohibited omissions of material fact, without regard for reliance on the deception, or (b) have not addressed those issues.

78. Plaintiffs and the other members have suffered injury in fact and actual damages including lost money and property as a result of Michaels' violations of 815 ILCS 505/2.

79. Plaintiffs and the other Class members' injuries were proximately caused by Michaels' fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

80. By this conduct, Michaels violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of Illinois, or conflict with each other for purposes of this action.

COUNT III

Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act (In the alternative to Count II and on Behalf of the Illinois State Class)

81. Plaintiffs incorporate paragraphs 1-58 as if fully set forth herein.

82. Plaintiffs and the other members of the Class were deceived by Michaels' failure to properly implement adequate, commercially reasonable security measures to protect their private financial information while shopping at Michaels.

83. Michaels intended for Plaintiffs and the other members of the Class to rely on Michaels to protect the information furnished to it in connection with their debit and credit card transactions, in such manner that the transactions would be protected, secure, and not susceptible to access from unauthorized third parties.

84. Michaels instead handled Plaintiffs and the other Class members' personal information in such manner that it was compromised.

85. Michaels failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

86. It was foreseeable that Michaels' willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

87. Michaels benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Michaels saved on the cost of those security measures.

88. Michaels' fraudulent and deceptive acts and omissions were intended to induce Plaintiffs' and the other Class members' reliance on Michaels' deception that their financial information was secure and protected when using debit and credit cards to shop at Michaels.²²

89. Michaels violated 815 ILCS 505/2 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs' and the other members' private financial information, by failing to warn shoppers that their information was at risk, and by failing to immediately notify affected customers of the nature and extent of the security breach.

90. Michaels' acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

91. Michaels' conduct constitutes unfair acts or practices as defined in that statute because Michaels caused substantial injury to Class members that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

92. In addition, Michaels also engaged in an unlawful practice by failing to comply with 815 ILCS 530/10(a), which provides:

²² The consumer protection statutes or interpretive law of the Consumer Fraud States have also either: (a) expressly prohibited omissions of material fact, without regard for reliance on the deception, or (b) have not addressed those issues.

Sec. 10. Notice of Breach. (a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system

93. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 “constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.”

94. Plaintiffs and the other members have suffered injury in fact and actual damages including lost money and property as a result of Michaels’ violations of 815 ILCS 505/2.

95. Plaintiffs and the other Class members’ injuries were proximately caused by Michaels’ fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

COUNT IV

Violation of New York General Business Law

(In the alternative to Count II and on behalf of the New York State Class)

96. Plaintiffs incorporate paragraphs 1-58 as if fully set forth herein.

97. New York General Business Law (“GBL”) § 349 makes unlawful “[d]eceptive acts or practices in the conduct of any business, trade or commerce.” N.Y. Gen. Bus. Law § 349.

98. Defendant’s transactions with Plaintiffs and the Class as described herein constitute the “conduct of any trade or commerce” within the meaning of GBL § 349.

99. Defendant in the normal course of its business collected customer information.

100. Michaels violated GBL § 349 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiffs’ and the other members’ private financial information, by failing to warn shoppers that their information was at risk, and by

failing to immediately notify affected customers of the nature and extent of the security breach. Defendant misrepresented the safety and security of their payment systems, and the unauthorized collection and storage of customer financial information beyond the immediate transaction.

101. Plaintiffs and the other members have suffered injury in fact and actual damages including lost money and property as a result of Michaels' violations of GBL § 349.

102. Plaintiffs' and the other Class members' injuries were proximately caused by Michaels' fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Michaels, as follows:

- A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives and appointing the undersigned counsel as Class Counsel for the Class;
- B. Ordering Michaels to pay actual damages to Plaintiffs and the other members of the Class;
- C. Ordering Michaels to pay for not less than three years of credit card monitoring services for Plaintiffs and the other members of the Class;
- D. Ordering Michaels to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;
- E. Ordering Michaels to pay statutory damages, as provided by the Illinois Consumer Fraud and Deceptive Business Practices Act, New York General Business Law § 349, and other applicable State Consumer Fraud Acts, to Plaintiffs and the other members of the Class;

- F. Ordering Michaels to disseminate individualized notice of the Security Breach to all Class members and to post notice of the Security Breach in all of its affected stores;
- G. Ordering Michaels to pay attorneys' fees and litigation costs to Plaintiffs and the other members of the Class;
- H. Ordering Michaels to pay both pre- and post-judgment interest on any amounts awarded; and
- I. Ordering such other and further relief as may be just and proper.

Dated: May 7, 2014

Respectfully submitted,

CHRISTINA MOYER, MICHAEL C. GOUWENS,
JESSICA E. GOUWENS, NANCY MAIZE,
JESSICA GORDON, DANIEL RIPES, and MARY
JANE WHALEN, individually and on behalf of all
others similarly situated

/s/ Joseph J. Siprut

Joseph J. Siprut
jsiprut@siprut.com
Melanie K. Nelson
mnelson@siprut.com
Gregg M. Barbakoff
gbarbakoff@siprut.com
Gregory W. Jones
gjones@siprut.com
SIPRUT PC
17 North State Street
Suite 1600
Chicago, Illinois 60602
312.236.0000
Fax: 312.267.1906

/s/ Daniel A. Edelman

Daniel A. Edelman
courtecl@edcombs.com
Cathleen M. Combs
ccombs@edcombs.com
Dulijaza Clark
jclark@edcombs.com
James O. Latturmer
jlatturmer@edcombs.com

Rebecca A. Cohen
rcohen@edcombs.com
EDELMAN, COMBS, LATTURNER & GOODWIN LLC
120 S. LaSalle
Suite 1800
Chicago, Illinois 60603
312.739.4200
Fax: 312.419.0379

*Plaintiffs' Interim
Co-Lead Counsel*

Mark T. Lavery
mark@lifetimedebtsolutions.com
HYSLIP & TAYLOR LLC LPA
917 W. 18th Street
Suite 200
Chicago, Illinois 60608
312.508.5480

Christopher V. Langone
207 Texas Lane
Ithaca, NY 14850
607.592.2661

Katrina Carroll, Esq.
kcarroll@litedepalma.com
LITE DEPALMA GREENBERG, LLC
Chicago Office
One South Dearborn
Suite 2100
Chicago, Illinois 60603
312.739.4200
Fax: 312.419.0379

Robert Ahdoot
rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, P.C.
1016 Palm Avenue
West Hollywood, CA 90069
310.474.9111
Fax: 310.474.8585

John A. Yanchunis
jyanchunis@forthepeople.com
**MORGAN & MORGAN COMPLEX LITIGATION
GROUP**
201 North Franklin Street, 7th Floor
Tampa, FL 33602
813.275.5272
Fax: 813.226.5402

Brian Murray
bmurray@glancylaw.com
GLANCY, BINKOW & GOLDBERG LLP
122 E 42nd Street, Suite 2920
New York, NY 10168
212.682.5340
Fax: 212.884.0988

Plaintiffs' Executive Committee

Richard R. Gordon
richard.gordon@gordonlawchicago.com
GORDON LAW OFFICES, LTD.
211 West Wacker Drive
Suite 500
Chicago, Illinois 60606
312.332.5200
Fax: 312.236.7727

Additional Plaintiff's Counsel of Record

CERTIFICATE OF SERVICE

The undersigned, an attorney, hereby certifies that a true and correct copy of the foregoing **Consolidated Class Action Complaint** was filed on May 7, 2014 via the electronic filing system of the Northern District of Illinois, which will automatically serve all counsel of record.

/s/ Joseph J. Siprut

Joseph J. Siprut

4816-0715-8554, v. 2